116TH CONGRESS
1ST SESSION

S. 1808

To require the Secretary of State to design and establish a Vulnerability Disclosure Process to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of Internet-facing information technology of the Department of State, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 12, 2019

Mr. GARDNER (for himself and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on Foreign Relations

---

A BILL

To require the Secretary of State to design and establish a Vulnerability Disclosure Process to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of Internet-facing information technology of the Department of State, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Hack Your State Department Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) BUG BOUNTY PROGRAM.—The term ''bug bounty program'' means a program under which an approved individual, organization, or company is temporarily authorized to identify and report vulnerabilities of Internet-facing information technology of the Department in exchange for compensation.

(2) DEPARTMENT.—The term ''Department'' means the Department of State.

(3) INFORMATION TECHNOLOGY.—The term ''information technology'' has the meaning given such term in section 11101 of title 40, United States Code.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of State.

(5) VDP.—The term ''VDP'' means the Vulnerability Disclosure Process established pursuant to section 3.

SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLOSURE PROCESS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall design, establish, and make publicly known a Vulnerability Disclosure Process to improve cybersecurity within the Department by—

(1) providing security researchers with clear guidelines for—

(A) conducting vulnerability discovery activities directed at Department information technology; and

(B) submitting discovered security vulnerabilities to the Department; and

(2) creating Department procedures and infrastructure to receive and fix discovered vulnerabilities.

(b) REQUIREMENTS.—In establishing VDP pursuant to subsection (a), the Secretary shall—

(1) identify which Department information technology should be included in the process;

(2) determine whether the process should differentiate among and specify the types of security vulnerabilities that may be targeted;

(3) provide a readily available means of reporting discovered security vulnerabilities and the form in which such vulnerabilities should be reported;

(4) identify which Department offices and positions will be responsible for receiving, prioritizing, and addressing security vulnerability disclosure reports;

(5) consult with the Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the VDP requirements are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law for specific activities authorized under VDP;

(6) consult with the relevant offices at the Department of Defense that were responsible for launching the 2016 Vulnerability Disclosure Program, ''Hack the Pentagon'', and subsequent Department of Defense bug bounty programs;

(7) engage qualified interested persons, including nongovernmental sector representatives, about the structure of VDP, as constructive and to the extent practicable; and

(8) award contracts to entities, as necessary, to manage VDP and implement the remediation of discovered security vulnerabilities.

(c) ANNUAL REPORTS.—Not later than 180 days after the establishment of VDP under subsection (a) and annually thereafter for the following 6 years, the Secretary shall submit a report to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs

of the House of Representatives regarding the establishment of VDP, including information relating to—

(1) the number and severity, in accordance with the National Vulnerabilities Database of the National Institute of Standards and Technology, of security vulnerabilities reported through VDP;

(2) the number of previously unidentified security vulnerabilities remediated as a result of such reporting;

(3) the current number of outstanding previously unidentified security vulnerabilities and the Department's remediation plans to address such vulnerabilities;

(4) the average period between the reporting of security vulnerabilities and the remediation of such vulnerabilities;

(5) the resources, surge staffing, roles, and responsibilities within the Department used to implement VDP and complete the necessary security vulnerability remediation; and

(6) any other information that the Secretary determines to be relevant.

SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PROGRAM.

(a) ESTABLISHMENT OF PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary shall establish a Bug Bounty Pilot Program to minimize security vulnerabilities of Internet-facing information technology of the Department.

(2) REQUIREMENTS.—In establishing the pilot program under paragraph (1), the Secretary shall—

(A) provide compensation for reports of previously unidentified security vulnerabilities within the websites, applications, and other Internet-facing information technology of the Department that are accessible to the public;

(B) award contracts to entities, as necessary, to manage the pilot program and for executing the remediation of security vulnerabilities identified pursuant to subparagraph (A);

(C) identify which Department information technology should be included in the pilot program;

(D) consult with the Attorney General on how to ensure that individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law for

specific activities authorized under the pilot program;

(E) consult with the relevant offices at the Department of Defense that were responsible for launching the 2016 ''Hack the Pentagon'' pilot program and subsequent Department of Defense bug bounty programs;

(F) develop a process by which an approved individual, organization, or company can—

(i) register with entities referred to in subparagraph (B);

(ii) submit to a background check, as determined by the Department; and

(iii) receive a determination as to eligibility for participation in the pilot program;

(G) engage qualified interested persons, including nongovernmental sector representatives, about the structure of the pilot program, as constructive and to the extent practicable; and

(H) consult with relevant United States Government officials to ensure that the pilot program complements persistent network and vulnerability scans of the Department's Inter-

net-accessible systems, such as the scans conducted pursuant to Binding Operational Directive 15–01, issued by the Secretary of Homeland Security on May 21, 2015.

(3) DURATION.—The pilot program established under paragraph (1) should be terminated not later than 1 year after the date on which it is established.

(b) REPORT.—Not later than 180 days after the completion of the Bug Bounty Pilot Program under subsection (a), the Secretary shall submit a report to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives that describes the pilot program, including information regarding—

(1) the number of approved individuals, organizations, or companies involved in the pilot program, broken down by—

(A) the number of approved individuals, organizations, or companies that registered for the pilot program;

(B) the number of such entities that were approved to participate in the pilot program;

(C) the number of such entities that submitted security vulnerabilities under the pilot program; and

(D) the number of such entities that received compensation under the pilot program;

(2) the number and severity, in accordance with the National Vulnerabilities Database of the National Institute of Standards and Technology, of security vulnerabilities reported under the pilot program;

(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

(4) the current number of outstanding previously unidentified security vulnerabilities and the Department's plans for remediating such vulnerabilities;

(5) the average period between the reporting of security vulnerabilities and the remediation of such vulnerabilities;

(6) the types of compensation provided under the pilot program; and

(7) the lessons learned from the pilot program.

○